CLAIMS

1. A method for customizing a set (S) of several second security units (EI), comprising secure downloading of an application key (TA) from a first security unit (AS) of a central processing unit to said set of second security units (EI), said first unit and second units each comprising at least one memory (M), characterized in that it comprises the steps of:

for each second unit (EI) in said set (S),

- on each downloading, computing an operation key (T1) in the first unit (AS) based on information specific to the second unit (EI), a transport key (T), and a diversification algorithm (ALGO1), said transport key (T) residing within the memory (M) of the first security unit (AS), said memory (M) being non-volatile,

- encrypting the application key (TA) in the first unit (AS) based on information comprising said operation key (T1) and an encryption algorithm (ALGO2), said application key (TA) residing in said memory (M),

- sending data (DATA) comprising the encrypted application key (TA) to the second unit (EI),

- on each downloading, computing an operation key (T1) in the second unit (EI) based on information specific to the second unit (EI), the transport key (T) and the diversification algorithm (ALGO1), the same transport key (T) residing in the non-volatile memory (M) of each second security unit (EI) of said set (S), said operation key (T1) not being stored within the memory (M) of said second unit,

- decrypting the encrypted application key (TA) in the second unit (EI) based on information comprising said operation key (T1) and a decryption algorithm (ALGO2P) which is the inverse of the encryption algorithm (ALGO2).

2. A method according to claim 1, characterized in that it further comprises an additional step of:

Sub A2

- sending information specific to the second unit (EI) to the first unit (AS) before computing the application key (T1) in the first unit (AS).

3. A method according to claims 1 or 2, characterized in that it further comprises an additional step of:

- sending a random number provided by the second unit (EI) to the first unit (AS), before encrypting the application key (TA) in the first unit (AS).

4. A method according to any of the preceding claims, characterized in that it further comprises an additional step of:

- sending information pertaining to an application key (TA) to the first unit (AS), before encrypting the application key (TA) within said unit (AS).

5. A method according to claim 4, characterized in that it further comprises an additional step of:

- choosing the application key (TA) to be encrypted based on said information.

6. A method according to any of the preceding claims, characterized in that said encryption of an application key (TA) intended for a second unit (EI) is unique.

7. A method according to any of the preceding claims, characterized in that it further comprises an additional step of:

- verifying integrity of the data (DATA) include the encrypted application key (TA).

Sub A2

8. A method according to any of the preceding claims, characterized in that it further comprises an additional step of:

- sending information pertaining to an application key (TA) to the second unit (EI), before decrypting the encrypted application key (TA) within said unit (EI) of said set (S).

9. A method according to any of the preceding claims, characterized in that it further comprises an additional step of:

- storing within the second unit (EI), after decrypting the encrypted application key (TA), said key (TA) within said unit (EI).

10. A method according to claim 9, characterized in that storing of the application key (TA) within the second unit (EI) is done based on information pertaining to an application key (TA).

11. A method according to any of the preceding claims, characterized in that it further comprises an additional step of:

- verifying that the application key (TA) is authentic.

12. A method according to any of the preceding claims, characterized in that the first security unit (AS) is a smart card.

13. A method according to any of the preceding claims, characterized in that the memory (M) is a rewritable memory.

14. A method according to any of the preceding claims, characterized in that a second unit (EI) comprises several application keys (TA).

15. A method according to any of the preceding claims, characterized in that the first unit (AS) comprises several application keys (TA).

16. A method according to any of the preceding claims, characterized in that it further comprises an additional step of:

- after encrypting the application key (TA), erasing the operation key (T1) temporarily saved within the second volatile memory of the first unit (AS).

17. A method according to any of the preceding claims, characterized in that it further comprises an additional step of :

- after decrypting the application key (TA), erasing the operation key (T1) temporarily saved within a second volatile memory (M2) in the first unit (EI).

18. A method according to preceding claims 2 to 4, characterized in that it further comprises an additional step of:

- sending the random information, information (REF1) pertaining to an application key (TA) and information (SN) specific to the second unit (EI) to the first unit (AS) by means of a first single command (EXPORTKEY).

19. A method according to preceding claims 1 and 2, characterized in that it further comprises the additional steps of:

- sending the encrypted application key (TA) and the information (REF2) pertaining to an application key (TA) to the second unit (EI) by means of a single second command (IMPORTKEY).